Liiketoiminnan jatkuvuuden hallintajärjestelmän kehitys asiakasyritykselle

Juuso Hirsmäki

2020 Laurea

Laurea-ammattikorkeakoulu

Liiketoiminnan jatkuvuuden hallintajärjestelmän kehitys asiakasyritykselleLiiketoiminnan jatkuvuuden hallintajärjestelmän kehitys asiakasyritykselle

Tietojenkäsittely
Opinnäytetyö
Toukokuu
2020

Laurea-ammattikorkeakoulu **Tiivistelmä**
Opinnäytetyö
Tradenomi (AMK)

Juuso Hirsmäki

Liiketoiminnan jatkuvuuden hallintajärjestelmän kehitys asiakasyritykselle Liiketoiminnan jatkuvuuden

2020 2020 Sivumäärä 48

Opinnäytetyön tavoitteena oli rakentaa osittain valmis liiketoiminnan jatkuvuuden hallintajärjestelmä asiakasyritykselle. Yrityksellä ei ole projektin valmistumisen aikana jatkuvuuden hallintajärjestelmän prosessiomistajaa, minkä vuoksi osa yrityksen sisäisistä linjauksista tullaan päättämään myöhemmin. Yritys haluaa pysyä nimettömänä. Viitekehyksenä on suuryrityksen tietohallinto, standardit, liiketoiminnan jatkuvuus ja prosessikehitys.

Yritykseltä löytyy paljon teknisiä tietoturvajärjestelmiä ja sen ylläpitoon liittyviä kontrolleja ja prosesseja. Tästä huolimatta yrityksen tietohallinnassa on keskityttävä laajempaan kokonaiskuvaan yrityksen liiketoiminnan jatkuvuudesta ja mitä riskimaisemaan liiketoiminnan kannalta saattaa kuulua.

Yrityksen vuoden 2018 tilaa arvioidessa käytettiin Gap-analyysia selvittäessä yrityksen sen hetkisen tilan ja kehitysprojektilla saavutetun tilan eroavaisuuden. Näiden kahden tilan välille suunniteltiin korkean tason tehtävät Gantt-kaavioon. Nykytilan kartoitukseen käytettiin myös soveltuvuuslausuntoa, joka pohjautui yrityksen kannalta oleellisiksi valittuihin ISO 22301 -kontrolleihin. Kontrollien valinta perustui yrityksen tilaan vuonna 2018. Soveltuvuuslausunnolla pystyttiin mittaamaan yrityksen valmiutta ISO 22301 -standardin sertifioinnille.

Työssä selvitettiin, miltä osin uusi versio ISO 22301:2019 on tuonut standardiin muutoksia ja mitä tulee ottaa huomioon standardin hakuvaiheessa. Työ ja tehty analyysi perustuvat vanhempaan ISO 22301:2012-versioon. ISO 22301 -standardi perustuu aikaisempiin BS 25999-1-ja BS 25999-2 -standardeihin vuosilta 2006 ja 2007.

Lopputuote on liiketoiminnan jatkuvuuden hallintajärjestelmän runko ja nykytilan arvio yrityksen kypsyydestä auditoinnille ja sertifioinnille ISO 22301:2012 -standardin mukaan. Työhön sisältyy valmiita hallintajärjestelmän dokumentaatiopohjia, joita yritys voi halutessaan ottaa käyttöön prosessiomistajan löydyttäessä. Opinnäytetyön ja sen analytiikan tarkoituksena on herättää pohdintaa toimialojen jatkuvasti muuttuvasta riskimaisemasta ja valmistaa yritys tekemään oikeat ratkaisut prosessin jalkautusvaiheessa. Tehdyistä analyyseista ja liiketoiminnan jatkuvuuden hallintajärjestelmän rungosta on osattava valita ne osa-alueet, joita halutaan hyödyntää ja miltä osin riskimaiseman arvio on tehtävä uudelleen.

Asiasanat: Liiketoiminnan jatkuvuussuunnitelma, Hallintajärjestelmä, Toimintamallit, Auditointi, Standardit, ISO 22301

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology

Juuso HirsmäkiJuuso Hirsmäki

Development of a Business Continuity Management System for a Company

2020 2020 Pages 48

The purpose of this thesis was to develop a partially complete Business Continuity Management System, (later BCMS) for the commissioner. The company does not have a BCMS process owner at the time of this thesis project, therefore some of the internal processes and policies will be decided later and not during this thesis project. The goal is to provide a good head start for the future process development and implementation. The frame of reference is corporate information management, standards, business continuity and process development. The company wants to remain anonymous.

The company has many technical information security systems and controls in place and its overall information security is well thought of, but the best practice is to have a broader picture of the overall business continuity management and the risk landscape regarding it.

The research methods used in this thesis consist of Gap analysis and Gantt chart. The methods also included a review and analysis of the current state of the company and the results were compared to the Statement of Applicability (later SoA). The SoA was based on the ISO 22301 controls that were selected to be relevant for the company and its current state in 2018.

The end user product was a frame of partially ready management system and evaluation of the maturity of the company's readiness for ISO 22301 auditing and acquisition of the respected standard. The product includes a ready-made analysis and framework done in 2018 and 2019. This can be used in the future when the BCMS process owner is selected. The thesis itself and the analysis that was conducted has a purpose to stimulate awareness and reflection of the industries ever-changing risk landscape and to make decisions based on the current landscape in the process building and implementation phase whenever that may be. The client (or end user) must stay critical regarding which analyses to keep and from what viewpoint the risk landscape analysis shall be updated accordingly.

This thesis also examines the newly introduced changes to the ISO 22301 standard published in 2019, and what needs to be considered when applying for the standard in near future. This thesis and the project are based on the older version, ISO 22301:2012 standard. ISO 22301 - family is based on the previous British Standard BS 25999-1 and BS 25999-2 from 2006 and 2007.

Keywords: Business Continuity Management System, BCMS, BCP, ISO 22301, Industry best practices, Standards, Auditing

EU	**European Union**
BCMS	**Business Continuity Management System**
BCP	**Business Continuity Plan**
BC	**Business Continuity**
BC Council	**Business Continuity Council**
BIA	**Business Impact Analysis**
CIO	**Chief Information Officer**
COOP	**Continuity of Operations Planning**
DR	**Disaster Recovery**
IS Council	**Information Security Council**
ISMS	**Information Security Management System**
ISO 22301	**European Standard EN ISO 22301:2014 ”Societal security. Business continuity management systems. Requirements (ISO 22301:2012)”**
ISO 27001	**ISO/IEC 27001 Information Security Management**
ISSO	**Information Systems Security Officer**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
PDCA	**Plan, Do, Check, Act**
POC	**Proof Of Concept**
RPO	**Return Point Objective**
RTO	**Return Time Objective**
SO	**Service Owner**

Sisällys

1 Johdanto 7
1.1 Kohdeyrityksen kuvaus 7
1.2 Yrityksen tausta 7
1.3 Tavoitteet 8
2 Teoreettinen viitekehys ja soveltavuusala 8
2.1 ISO 22301 standardi 8
2.1.1 Statement of Applicability - Soveltuvuuslausunto 9
2.2 Business Continuity Management System -Liiketoiminnan jatkuvuuden hallintajärjestelmä 9
2.2.1 Business Continuity Plan -Liiketoiminnan jatkuvuussuunnitelma 11
3 Projektin suunnittelu 12
3.1 Gap -analyysi ja Gantt -kaavio 12
4 Haastattelu ja jatkotoimenpiteet 13
4.1 Prosessikehitys 15
5 Tulokset yrityksen valmiusasteesta 16
5.1 Havainnoinnin tulokset 18
6 Johtopäätökset/pohdinta 19
6.1 Jatkotoimenpiteet 19
6.2 Valittu viitekehys 20
6.3 Omat tavoitteet 20
6.4 Projektin loppuunsaattaminen ja prosessin käynnistäminen 20

1 Johdanto

1.1 Kohdeyrityksen kuvaus

Yritys on yksi Euroopan johtavia teknisten ratkaisujen tarjoajia. Se suunnittelee, toteuttaa, huoltaa ja ylläpitää käyttäjäystävällisiä ja energiatehokkaita teknisiä ratkaisuja kiinteistöille, teollisuudelle ja infrastruktuurille.

Yhtiön vuoden 2018 liikevaihto oli noin 2,2 miljardia euroa ja yritys työllistää noin 15 000 työntekijää 12 toimintamaassa. Työni sijoittui Group IT osastolle, joka hallinnoi kansainvälisen yrityksen kaikkia tietoteknisiä ratkaisuja, tästä syystä kaikki yritykselle toimitettavat liitteet ovat englanniksi.

1.2 Yrityksen tausta

Tarve työlle nousi vuonna 2018 tehdystä projektista, jossa auditointiin yritystä ISO 27001 tietoturva standardia varten. Tuolloin standardin yhtenä osana oli arvioida tarve liiketoiminnanjatkuvuussuunnitelmalle. Huomattiin, että yrityksellä on lukuisia teknisiä tietoturva kontrolleja ja prosesseja käytössä. ISO 27001 projektin yhtenä tuotoksena oli täydellinen tietoturvan hallintajärjestelmä, Information Security Management System (ISMS). Tästä huolimatta puuttui yleisempi jatkuvuussuunnitelma ja sen hallintajärjestelmä.

Ongelmana oli siis, yhden kriittisen, alan parhaiden toimintamallien mukaisen liiketoiminnan jatkuvuuden hallintajärjestelmän puuttuminen. Yksinomaa pelkät IT ja tietoturva kontrollit eivät turvaa laaja-alaisempaa liiketoiminnan jatkuvuutta. ISO 27001 projektin puolelta tuli tarve Business Continuity Plan (BCP), mutta erillinen liiketoiminnan jatkuvuussuunnitelma ei takaa laajempaa kontrollia yrityksen kokonaisvaltaisesta liiketoiminnan hallinnasta.

Vuonna 2018 tehty auditointi ja standardinhakuprosessi ei vaatinut yleisen jatkuvuussuunnitelman olevan käytössä yrityksellä. Tuohon aikaan vuonna 2018 ISO 27001 -projektin ollessa loppusuoralla, alettiin käymään yrityksen sisäistä keskustelua tarpeesta liiketoiminnan jatkuvuuden hallintajärjestelmästä. Kun kyseessä on kansainvälinen suuryritys, on ilmeistä, että uuden yrityksen sisäisen prosessin kehitys ja jalkautus ei ole yhden henkilön mahdollista suorittaa työmäärän takia. Opinnäytetyö myös sijoittui aikavälille, jolloin en enää työskentelisi asiakasyrityksessä ja hallintajärjestelmän täydellinen pystytys ja prosessin käynnistäminen olisi vaatinut tiivistä yhteistyötä asiakasyrityksen kanssa, mutta koska yrityksellä ei vielä tuohon aikaan ollut liiketoiminnan jatkuvuuden hallintajärjestelmän prosessi omistajaa, en monia yrityksen sisäisiä päätöksiä hallintajärjestelmän pystytyksen suhteen voinut tehdä.

1.3 Tavoitteet

Edeltävistä syistä sovimme jo projektin alkuvaiheessa, että päämääränä ei ole tehdä täydellistä hallintajärjestelmää vaan tuottaa juostava runko, jota voidaan tarpeen tullen lähteä jatkokehittämään yrityksen sen hetkisen tilanteen ja tarpeiden mukaan. Lopullinen liiketoiminnan hallintajärjestelmän runko on dokumentaatio kokonaisuus opinnäytetyön liitetiedostona.

Toisena päätavoitteena oli tuottaa yrityksen ylimmälle johdolle arvio standardin auditointi valmiudesta. Tilaus oli konkreettiselle valmiusasteen arvioinnille numerona, jota yrityksen ylin johto halusi. Tästä olisi mahdollista rakentaa business case, jotta projektin loppuunsaattamiselle voitaisiin tehdä tarkempia arvioita. Tätä tilausta lähestyin rakentamalla ISO 27001 mallin mukaan soveltuvuuslausunnon, mikä oli räätälöity kohdeyrityksen viitekehykseen.

Kolmantena tavoitteena oli löytää kehitettäviä osa-alueita yrityksestä. Tätä lähestyin tuottamalla haastattelun ja tekemällä havaintoja yrityksen sisäisistä prosesseista vielä sillä aikaa, kun työskentelin heille. On huomioitava, että jos vuonna 2018 tehdyn haastattelun ja sen pohjalta tehdyn analyysin olisi käytetty sellaisenaan, voi riskimaisema muuttua kriittisessä määrin siten, että sen joustamattomuuden ja vanhan analytiikan takia hallintajärjestelmässä olisi puutteita tai se ei olisi nykytilaan soveltuva.

2 Teoreettinen viitekehys ja soveltavuusala

2.1 ISO 22301 standardi

ISO 22301:2012 standardi on valittu tietoperustaksi syystä, että se sisältää alan parhaaksi todettuja toimintamalleja ja kontrolleja. EU pohjaisille standardeille on myös helpompi löytää sertifioitu pääauditoija verrattuna esimerkiksi yhdysvaltalaiseen Continuity of Operations Planning (COOP). Valintaa COOP ja ISO 22301 väliltä pohdin lisää kappaleessa 6.

ISO 22301 on yrityksille parhaiksi toimintamalleiksi havaittuja käytäntöjä, joista vuosien kehityksen saatossa määritellään standardi. Näitä standardeja voidaan auditoida, jolloin puhutaan yrityksen standardin sertifiointi prosessista. ISO 22301 dokumentaatio sisältää ohjeistusta yrityksen liiketoiminnan jatkuvuuden hallintajärjestelmän pystyttämiselle.

Rhand Leal kertoo blogi kirjoituksessaan uuden ja vanhan standardin eroavaisuuksista. Yritykset, jotka on sertifioitu 2012 versioon tulee siirtyä 2019 versioon 31.10.2022 mennessä. 2012 sertifiointi tulee astumaan pois voimasta lokakuussa 2022. Uudessa standardi versiossa on

vähemmän dokumentoidun tiedon ja prosessien teknisiä vaatimuksia. Vanhassa standardissa kuvataan tarkemmin hallintajärjestelmän vaatimukset. (Rhand Leal 2019.)

Uusi 2019 versio sisältää uusia vaatimuksia;
Resurssit tunnistetaan ratkaisujen perusteella, muutoksista hallintajärjestelmään tulee ottaa huomioon mahdolliset seuraamuksen, eheys, resurssit ja vastuualueet. Vaikutustyypit ja konteksti oleelliset kriteerit ovat pakollisia yritystoiminnan vaikutus analyysissa. Uudessa standardi versiossa pääpainoa vanhasta strategia pohjaisesta toiminnasta siirretään ratkaisu pohjaiseen ajattelumalliin ja toimintaan.

2.1.1 Statement of Applicability - Soveltuvuuslausunto

BCMS SoA perustuu ISO 22301 kontrolleihin, joissa on maininta ”shall” tai kontrollille on asetettu vaatimus, että se tulee löytyä yritykseltä dokumentoituna tietona. Lisänä on myös muita valintoja, jotka näin oleelliseksi asiakasyrityksen tapauksessa.

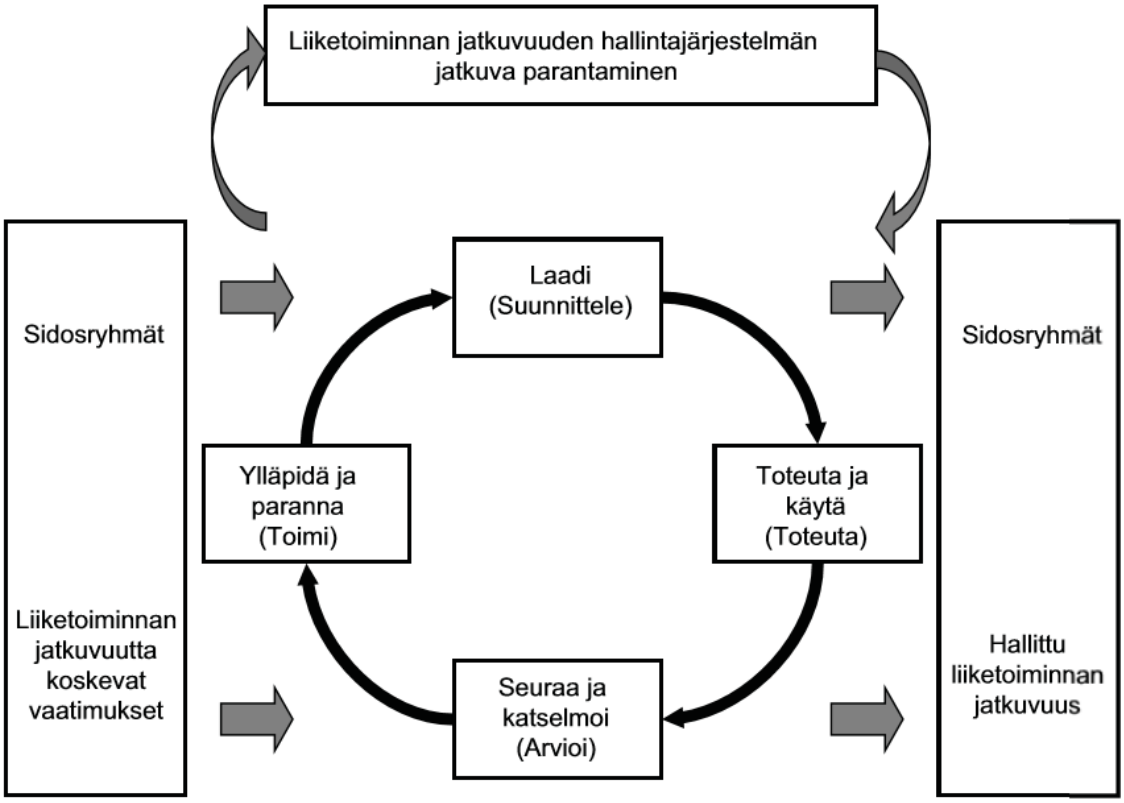
Soveltuvuuslausuntoon on listattu kaikki kohdat ISO 22301:2012 standardista, jossa kontrollista tai sen olemassaolosta on oltava dokumentoitua tietoa. ISO 22301 standardi ei tarjoa lisenssin ostajalleen valmista soveltuvuuslausuntoa samaan tapaa, kuin se on sisällytetty esimerkiksi ISO 27001 standardissa. Tämän takia tein oman soveltuvuuslausunto pohjan, johon keräsin dokumentoidun tiedon vaatimukset ja muut yritykselle ja sen viitekehykselle oleelliset kohdat, mitkä koskevat asiakasyritystä ja tuovat lisäarvoa soveltuvuuslausunnolle.

Yleisesti soveltuvuuslausunnon on tarkoituksena kehittää yrityksen auditointiprosessia ja parantaa liiketoiminnan jatkuvuuden hallintajärjestelmän tai muun standardin hallintajärjestelmän toimivuutta valitsemalla oikeat kontrollit ja prosessit oikeaan viitekehykseen. Projektissani soveltuvuuslausunto oli isossa osassa määrittää yrityksen valmiutta standardin dokumentaatio, kontrolli ja prosessien omaksumisen tasoa. Tästä pystyttiin määrittelemään yleinen valmiusaste jo olemassa olevan dokumentaatioiden ja kontrollien suhteen.

2.2 Business Continuity Management System -Liiketoiminnan jatkuvuuden hallintajärjestelmä

Hallintajärjestelmä kokonaisuuden ideana on jalkauttaa, ylläpitää ja jatkuvasti kehittää käytössä olevaa prosessia ja sen osioita. Hallintajärjestelmällä varmistetaan, että yrityksen taso noudattaa ja täyttää standardin vaatimukset auditointi ja sertifiointi vaiheessa täyttyvät ja tulevat täyttymään myös tulevaisuudessa, kun sertifikaatille haetaan tarkistusta.

Hallintajärjestelmä toimii taustalla pyörivien prosessien tukena ja virallistaa yrityksellä käytössä olevat toimintatavat, dokumentaation, koulutuksen, kommunikaation, mittarit, sisäisen auditoinnin ja varmistaa kokonaisuudessaan hallintajärjestelmän pysyvyyden standardin mukaisena ja yrityksen pyrkivän jatkuvaan kehitykseen, oman toiminnan mittaamiseen ja sen arviointiin. Kyseiseen jatkuvaan kehitykseen ja oman toiminnan arviointiin voi yritys käyttää esimerkiksi PDCA -menetelmän sykliä (Plan, Do, Check, Act). PDCA -menetelmä on ensimmäisenä suosituksena ISO 22301 standardissa.



Kuvio 1: PDCA -menetelmän sykli (ISO 22301)

Liiketoiminnan hallintajärjestelmän ideana on turvata yritystä sen sisäisten ja ulkoisten uhkien varalta. Ennaltaehkäisevän toiminnan lisäksi on tarkoituksena turvata liiketoiminnalle ja sen jatkuvuudelle kriittiset prosessit, niin katastrofin kuin siitä palautumisen aikana. (Wikipedia.org 2020.)

Hallintajärjestelmä yrityksellä käytössä oleville prosesseille ja toimintamalleille on todettu olevan yritykselle paras käytäntö toteuttaa liiketoiminnan jatkuvuuden toteutuminen ja sen prosessien ajaminen. Näihin parhaisiin käytäntöihin päästään alan pitkän kehityksen ja lopulta tiettyjen toimintamallien standardisoimisen kautta. ISO 22301 standardin tarkoituksena on auttaa yritystä tekemään päätös millä tapaa he aikovat ajaa omaa liiketoiminnan jatkuvuutta, tähän ISO 22301 toteaa parhaaksi malliksi sopivan liiketoiminnan jatkuvuuden hallintajärjestelmä.

Opinnäytetyön liitteistä löytyy itse hallintajärjestelmä, BCMS ja liiketoiminnan jatkuvuuden suunnitelma, BCP. BCMS dokumentaatio kasaa ja kuvaa kaikki yrityksen valitsemat kontrollit, prosessit ja sisäpolitiikan. Se määrittää ja sisältää yrityksen korkeantason näkemyksen ja tehtävän, mitä hallintajärjestelmällä pyritään saavuttamaan. Joissain tapauksissa yritys määrittelee BCMS dokumentaation BCMS Scope -dokumentiksi, tämä kuvaa hyvin mitä dokumentti pitää sisällään, kuvauksen ja rajapinnat siitä, mitä hallintajärjestelmä on laajuudessaan ja mikä on soveltamisalan ulkopuolella.

BCMS käyttäjä on yrityksessä määritelty liiketoiminnan jatkuvuuden prosessin omistaja. BCMS dokumentaatio käytetään säännöllisesti johdonkatselmuksessa, niin vuotuisesti kuin myös jos hallintajärjestelmään tulee oleellisia muutoksia.

2.2.1 Business Continuity Plan -Liiketoiminnan jatkuvuussuunnitelma

BCP on laadittu ISO 22301:2012 pohjalta ja sen sisältö on pääosin minimi vaatimuksia mitä standardi vaatii liiketoiminnan jatkuvuussuunnitelmasta. Jatkuvuussuunnitelma sisältää korkeantason tehtävät mitä yrityksen tulee saattaa loppuun, jotta ensimmäinen versio (Proof of Concept, POC) voidaan jalkauttaa ja kierrättää johdon katselmuksessa.

BCP on yksi tärkeimmistä osista liiketoiminnan jatkuvuuden hallintajärjestelmää. Siinä määritetään yrityksen tavoitteet ongelmatilasta palautumiselle, näitä ovat esimerkiksi palautuspisteen tavoite ja palautumiseen kuluneen ajan tavoite (Recovery Point Objective, RPO ja Recovery Time Objective, RTO) PRO ja RTO on yrityksen oma valinta, mikä taso halutaan saavuttaa missäkin ajassa ongelmatilasta palautumiselle. RPO ja RTO pohjautuvat yrityksen korkeantason tehtävän ja näkemyksen saavuttamiseen (Mission, Vision).

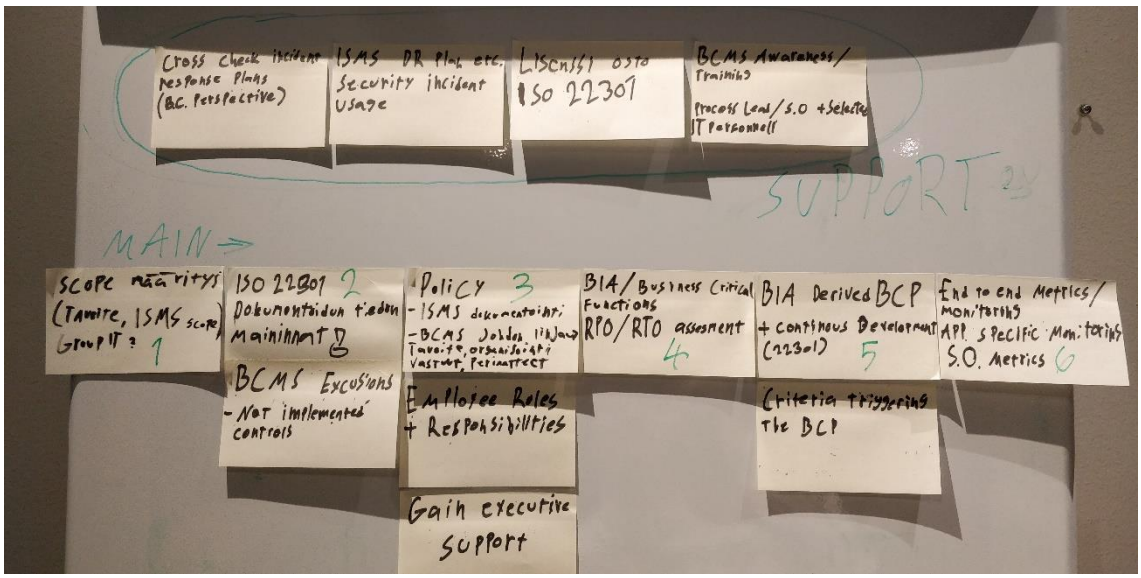
Oleellisena osana PRO ja RTO määrittelyttä on yrityksen tarkka riskimaiseman kartoitus ja hallintajärjestelmän tarkoituksen mukaisuuden määrittely. Tarkoituksen mukaisuuden määrittely on soveltamisalan määrittelyä. Tämän määrittyy BCMS Scope -dokumentaatio ja siihen kuuluva liiketoiminnan jatkuvuuden politiikka (BC Policy) mukaan. Politiikan määrittelyyn olisi tarvinnut yrityksen ylimmän johdon tiivistä yhteistyötä, joten oli löydettävä toinen keino, millä voisin kehittää mahdollisimman pitkälle liiketoiminnan jatkuvuussuunnitelmaa. Tämä toinen keino oli tarkoituksena olla tuotettu haastattelu ja sen tulokset, josta olisi saatu määriteltyä liiketoiminnan jatkuvuudelle oleellisia osia, niin kuin esimerkiksi RPO ja RTO. BCMS Policy ja selvän Scope -dokumentaation puuttuminen vaikeuttaa BCP -dokumentin luomista. Liitteistä löytyy BCP runko, jota on viety niin pitkälle kuin on ollut mahdollista.

3 Projektin suunnittelu

3.1 Gap -analyysi ja Gantt -kaavio

Päätin käyttää Gap -analyysiä projektin alkuvaiheessa määrittäessä yrityksen sen hetkistä tilaa ja toivottua kypsyysastetta, johon projektin oletetaan yltävän. Tässä opinnäytetyökonseptissa Gap -analyysillä on tarkoituksena määrittää, nimensä mukaisesti, kahden tilan välissä olevaa aukkoa. Tämän pohjalta määritellään, mitä aukon välille sisältyvät tehtävät tulisivat olemaa. Näin saadaan karkea tehtävälista tarvittavista toimenpiteistä, jotta haluttu tila saavutettaisiin. Tehtävälista jaotellaan mahdollisimman loogiseen järjestykseen ja ajoitetaan se halutulle aikavälille Gantt -kaavioon. Gap -analyysissä pääkohtia oli verrata käytössä olleita kontrolleja tai muita prosesseja, mitkä tukisivat liiketoiminnan jatkuvuuden hallintajärjestelmää.

Gap -analyysiin osallistui yrityksen Information Systems Security Officer (ISSO). Jaoimme tehtävät tuki- ja päätehtäviin. Kuvassa alhaalla näkyy tehdyn analyysin pohjalta laaditut tehtävät.



Kuvio 2: Korkeantason projektisuunnitelma.

Korkeantason tehtävät jaoin pienempiin osioihin, jotka merkitsin kalenteriin ajanjaksoille, jolloin pystyin muista työtehtävistäni antamaan aikaa opinnäytetyö projektille. Yrityksen työkoneelle rakensin korkeantason tehtävät Gantt -kaavion MS Outlook sovellukseen, jotta projektia oli helpompi seurata.

Analyysin päätuloksina oli, että monia jo käytössä olevia IT kontrolleja ja prosesseja pystyisi mainita ja sisällyttää tulevassa liiketoiminnan jatkuvuuden hallintajärjestelmässä. Tältä osin olimme hiukan samantyylisessä lähtöasetelmassa kuin aiemman ISO 27001 projektin suhteen. Hyväksi havaittuja kontrolleja ja prosesseja oli käytetty jo pitkään yrityksessä, mutta niitä ei ollut virallistettu tai dokumentoidu oikealla tavalla. Voitiin sanoa, että osa runkoa on olemassa, mutta liima puuttuu. Tuo kyseinen liima tulisi olemaan virallistettu ja dokumentoitu hallintajärjestelmä ja siihen kuuluvat erilliset prosessikuvaukset ja kaaviot, mitkä pitävät kokonaisuuden ja prosessin kasassa.

Prosessia on helpompi hallita, kun on selvästi määritelty politiikka ja rajapinnat, BCMS Scope -dokumentti ja BCMS Policy -dokumentti. Analyysissä kävi myös ilmi, että projektiin kuuluu vaiheita, joita en pysty tuottamaan itsekseni opinnäytetyö projektini aikana. Yhtenä esimerkkinä on yrityksen sisäpolitiikan laadinta hallintajärjestelmän suhteen (Policy dokumentti). Tämä on yrityskohtaista ja sisältää yleensä mission ja vision -tyylistä korkeantason linjausta, eli yrityksen korkeantason tehtävän ja näkemyksen laatiminen. Tähän tarvittaisiin yrityksen ylin johto mukaan prosessin pystytysvaiheessa.

Analyysin pohjalta voitiin todeta, että projekti tulisi vaatimaan valtavan määrän uutta dokumentaatiota yrityksen sisäisistä prosesseista ja toimintamalleista. Tämän lisäksi pelkkä dokumentointi ei riitä vaan prosessit on myös jalkautettava ja osasta niistä on löydyttävä myös näyttöä. Kyseinen dokumentointi ei ole täysin suoraviivaista, joitain yleisiä linjauksia pystyin tuottamaan ja antamaan suuntaviivoja hallintajärjestelmän suhteen. Isomman kaavan linjaukset ja suhteutus yrityksen senhetkiseen tilaan on tehtävä prosessin pystytys/standardin haku vaiheessa.

4 Haastattelu ja jatkotoimenpiteet

Haastatteluun osallistui yrityksen Information Systems Security Officer (ISSO) ja Chief Information Officer (CIO) rooleissa toimivat henkilöt. Kyselyn teetin pohjustamalla tilanteen mahdollisimman hyvin ja rakentamalla tietopohjan tarvittavista asioista. Liite tiedostona tuotettu kysely.

Haastattelun tutkimustuloksia ei ole hyödynnetty hallintajärjestelmän jatkuvuus suunnitelmaa laadittaessa. Tämä syystä, että riskimaisema vaihtuu vuosittain ja vanhoilla arvioilla ei voida toteuttaa yritystoiminnan vaikutusanalyysia (Business Impact Analysis, BIA). BIA ja sen määrittely on osa liiketoiminnan jatkuvuuden suunnitelmaa, BCP dokumenttia. Haastattelun tarkoituksena oli määritellä yrityksen riskimaisemaa ja kehittää sen pohjalta BCP -dokumenttia mahdollisimman pitkälle. Tuloksia ei ole hyödynnetty alhaisen osallistumisprosentin ja vanhentuneen analytiikan takia. Haastatteluosio on kuitenkin sisällytetty opinnäytetyössä, koska

käytettyä haastattelupohjaa ja sen skenaarioita voidaan hyödyntää myöhemmässä vaiheessa, kun projektia viedään loppuun.

Tulosten vanhentuessa ja vastausprosentin alhaisuuden myötä en antanut suurta painoarvoa tuotetulle kyselylle. Yhdeksästä haastateltavasta kaksi henkilöä antoi vastaukset, joka johtaa 22% vastausprosenttiin. Kysely tulisi tuottaa uudelleen yrityksen sisäisesti kaikille osastoille prosessin pystytysvaiheessa, jolloin saavutetaan ajantasainen ja tarkka riskimaisema. Jos riskimaisema muodostettaisiin kahden vastanneen henkilön perusteella, voisi kuva mahdollisista riskeistä vääristyä, koska arviointi perustuisi vain kahden ihmisen näkemykseen yrityksen osa-alueista. Tämän takia kysely tulisi tuottaa uudelleen korkeammalla vastausprosentilla ja laajemmalla hajonnalla. Alkuperäiseen kyselyyn oli määrä osallistua yrityksen eri osastoista henkilöitä ja prosessi vastaavia. Näitä olivat;

- *Head of Enterprise Architecture and demand*
- *Head of Development and Operations*
- *Head of Project Management Office, T&T*
- *Senior Manager, Applications*
- *IT Manager, IT Infrastructure*
- *Senior manager, Enterprise Architecture & process demand*
- *Head of People Processes and Solutions*
- *Chief Information Officer*
- *Information Systems Security Officer*

Kyseinen otanta olisi ollut kattava, jos kaikki yllä mainitut henkilöt olisivat osallistuneet haastatteluun. Parhaaseen tulokseen päästäisiin pitämällä Business Continuity council, samalla tapaa kuin yrityksessä pidetään Information Security council (IS Council). Yrityksellä on tapana pitää vuotuinen tietoturva riskien kartoitus, johon osallistuu suuri määrä henkilöitä yrityksen eri osa-alueilta. IS Council on laajempi palaveri, johon osallistui laajin havaitsemani otanta yrityksen eri osastoista ja prosessivastaavista. Tällä kyseisellä kokoonpanolla ja council tyylisellä konseptilla olisi mahdollista tuottaa tarkka riskimaisema myös liiketoiminnan jatkuvuuden suunnittelun aikana. Ehdotukseni on, että samantyylinen toimintatapa otetaan käyttöön myös liiketoiminnan jatkuvuuden kehityksessä samalla tapaa, kuin sitä käytetään tietoturva riskien ja tietoturvan kehityksessä IS Council palavereissa.

4.1 Prosessikehitys

Toteutetusta haastattelusta irrallisena keskusteluna kävimme pohdintaa työntekijän työtehokkuuden parantamisesta. Tässä kontekstissa ei viitattu työntekijän yksilöllisiin vaikutteisiin, esimerkiksi työstressiin tai motivaation puutteeseen vaan työntekijälle ulkoiset tekijät, joihin hän ei itse voi vaikuttaa. Näitä voi olla esimerkiksi huonosti toimiva yrityksen sisäinen prosessi, jonka takia työtehtävät ja projektit viivästyvät.

Haastatellessani yrityksen henkilöitä tähän näkökulmaan tuli vastaus, että kyseinen lisäys olisi tärkeä, koska se tukisi yrityksen jo olemassa olevaa ajattelumallia, jonka mukaan:

”Työntekijän kokemus tietohallinnon palveluista voi johtua yhdestä huonosti toimivasta komponentista ja sitä ei korvaa monta muuta toimivaa asiaa, jos henkilö ei saa töitään tehtyä.”
-Yrityksen Information Systems Security Officer, ISSO.

Havainto keskittyi yrityksen toimintatapoihin ja sisäisiin prosesseihin. Näitä pidin silmällä sen aikaa, kun työskentelin yrityksessä. Työpisteeni oli viereinen työpiste yrityksen teknisen tuen työpisteestä. Tämän takia huomasin, että yrityksen eri osa-alueilta saattoi päivän aikana käydä useaan kertaan kysymässä teknistä tukea, mitä ei ollut mahdollista saada, jos tukihenkilö ei ollut sinä päivänä paikalla. Tukihenkilön saatavuus määräytyi ennalta asetetun kiertävän tuen mukaan. Yksi tukihenkilö oli vastuussa yrityksen monesta eri toimipisteestä. Havaintoon kuului myös avointa keskustelua, joissa kävi ilmi työntekijöiden päivittäiset vastoinkäymiset.

5 Tulokset yrityksen valmiusasteesta

Soveltuvuuslausunnon mukaan dokumentaation kypsyys on opinnäytetyöprosessin loputtua 36%. Tähän tulee lisätä muut valitut kontrollit ja työ, mitä tarvittaisiin prosessin jalkauttamiselle yrityksessä. Lopullinen työmäärä huomioituna arvioin hallintajärjestelmän istuvan noin 25-35% valmiusasteessa, joten alkuperäisiin tavoitteisiin on päästy ja hallintajärjestelmän runko, dokumentaatio kokonaisuus on saatu valmiiksi. Tulokseen on päästy arvioimalla projektin aikana yllettyä kypsyyspistettä. Hallintajärjestelmä saavutti halutun kypsyyden ja tätä pistettä ja hallintajärjestelmän valmiutta on avioitu standardista tekemääni soveltuvuuslausuntoon. Soveltuvuuslausunto listaa tarvittavat kontrollit ja dokumentaation, jotta yritys voisi hakea standardin sertifiointia. Soveltuvuuslausunto ilmaisee dokumentaation valmiutta ja antaa yrityksen valmiudelle prosentuaalisen arvon. Tälle prosentti arvolle ei ollut ennalta määriteltyä tavoitetasoa, tavoitetaso oli saada hallintajärjestelmän runko valmiiksi ja arvio, kuinka pitkälle opinnäytetyö projekti yltää.

Dokumentaatiolle annoin prosentuaalisen arvon ja sen perusteella laskin kaikista vaadittavista kohdista keskiarvon. Laskukaavan löytää liitteistä soveltuvuuslausunnon Documentation maturity sivulta. Laskukaavan voi nähdä myös alla olevasta taulukosta. Arvion mukaan hallintajärjestelmän dokumentaatio osuus on noin 36 % valmis. Tähän lukuun on sisällytettävä muut kontrollit ja työ mitä soveltuvuuslausunto listaa. Lopullinen arvio on, että hallintajärjestelmä ja sen dokumentaation on 25-35% valmis. Tulos 36% valmiusasteesta kuvaa dokumentaatiokokonaisuuden valmiutta. Dokumentaatio kokonaisuus on tavoitteissa mainittu hallintajärjestelmän runko. Tavoitteita luodessa hallintajärjestelmän rungolle ei asetettu ennalta määritettyä valmiusastetta prosenttina, mihin sen tulisi yltää.

Documentation requirement	Status	
Legal and regulatory requirements, the organization shall establish, implement and maintain a procedure to identify, have access to, and assess the applicable legal and regulatory requirements	0%	Documentation missing
BCMS scope documentation	20%	Documentation missing, top level management decision/process owner proposal
BCMS Policy shall be available as documented information	0%	Will be included in BCMS documentation
Documented business continuity objectives	50%	Will be included in BCP documentation
Documented information of personnel competence	80%	Found in BCMS documentation
Documented information about documentation processes	80%	Will be included in BCMS documentation, version control, management review and approval cycle already in place
Control of documented information	70%	Will be included in BCMS documentation, version control, management review and approval cycle already in place
Keeping documented information about operational planning and processes to the extent necessary to have confidence that the processes have been carried out as planned	0%	Documentation missing
The organisation shall establish, implement and maintain a formal and documented process for business impact analysis and risk assessment that	80%	BCMS draft done + BCP
BIA, the organisation shall establish, implement and maintain a formal and documented evaluation process for determining continuity and recovery priorities, objectives and targets	80%	BCMS draft done + BCP
The organization shall establish, implement, and maintain a formal documented risk assessment process that systematically identifies, analyses and evaluates the risk of disruptive incidents to the organisation	60%	BCP documentation, BIA, TRA + BC Council?
The organisation shall document business continuity procedures (including necessary arrangements) to ensure continuity of activities and management of disruptive incident	40%	Documentation WIP
Incident response structure, the organisation shall establish, document, and implement procedures and management structure to respond to disruptive incident using personnel with the necessary responsibility, authority and competence to manage an incident	0%	Documentation missing
Recovery, the organisation shall have documented procedures to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident	0%	Documentation missing
Monitoring, measurement, analysis and evaluation, the organisation shall retain appropriate documented information as evidence of the monitoring and measurement results	0%	Documentation missing
Internal audit, Company shall retain documented information as evidence of the implementation of the audit programme and the audit results	0%	Documentation missing
Improvement, Nonconformities and corrective action. The organisation shall retain documented information as evidence of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action	60%	Corrective actions draft done
Average:	**36%**	

Taulukko1: Soveltuvuuslausunto

5.1 Havainnoinnin tulokset

Havaintoni työsuhteen aikana oli edellä mainittu kiertävän teknisen tuen konsepti. Tähän en täysin saanut varmistusta, kuinka paljon kyseinen kierto aiheuttaa ongelmia ja katkoksia työntekijätasolla, mutta oman havaintoni mukaan noin puolenvuoden aikana näin kaksi kyseistä tapausta, jossa työntekijä ei pystynyt suoriutumaan liiketoiminnan jatkuvuudelle kriittisestä tehtävästä. Näiden kahden tapauksen vaikutus on oletettavasti ollut normaalia työ viivästystä vakavampi. Kahden kriittisemmän havainnon lisäksi aiheutti kiertävä tuki useampaan kertaan edellisessä kappaleessa mainittuja B kategorian ongelmia. Työntekijän työtehokkuuden heikkeneminen, kun työntekijä ei ole kykenevä suorittamaan tehtäviään ja joutuu odottamaan kiertävää teknistä tukea. Havainto sijoittui hyvin pienelle alueelle yrityksen IT osastoa, joten otannassa ei ollut koko IT osasto mukana. Tämän perusteella arvioisin todellisen lukumäärän olevan noin 20+ kriittistä tapausta puolenvuoden ajalta, jos otantana on koko yrityksen suomen divisioona.

Kriittiseksi tapaukseksi lasken tilanteen, missä työntekijä ei pysty suorittamaan liiketoiminnalle kriittistä tehtävää, koska ei saa tarvittavaa IT tukea. Havainnon aikana oli useita tilanteita, missä henkilö olisi tarvinnut tukihenkilöä, muttei tarve ja tuen puute aiheuttanut kriittistä haittaa.

Toinen havainnoistani oli sähköisen roskapostin leviäminen. Kyseinen spam -roskaposti ei suoranaisesti estänyt työntekijätasolla työtehtävistä suoriutumista, mutta aiheuttaa tietyillä henkilöillä paljon ylimääräistä työtä. Tämä ylimääräinen työ on pois muusta yleisestä liiketoiminnasta ja täten tuottaa edellä mainittua vaikeasti mitattavaan yritystappiota. Jos roskapostin leviämistä ei saataisi yrityksen sisäverkossa kuriin, olisi yrityksen tietoturva henkilöstön resurssit sijoitettu kyseisen ongelman selvittämiseen, jolloin vakavampi tietoturvauhka saattaisi jäädä huomaamatta. Roskaposti sisälsi väärennettyjä laskuja ja jotkin henkilöt olivat maksaneet näitä liiketoiminnan puolella. Tämä on selvä tiedotuksen ja koulutuksen puute yrityksen sisällä. Asiasta tulisi tiedottaa hyvin tapahtuvan koulutuksen ja sisäisen kommunikaation ohella, jotta työntekijät tietäisivät, miten toimia epäilyttävien viestien suhteen.

Kahden havaintoni perusteella keskittyisin haravoimaan mahdollisimman tarkasti kaikki B -luokan tapahtumat ehdottamassani Business Continuity council -tilaisuudessa, johon kaikki yrityksen osasto osallistuisivat. Havaintojen pohjalta laadittaisiin hoitotoimenpiteet ja business case, joka antaisi yritysvoitto arvion tehdyistä toimenpiteistä. Tätä business case -arviota voitaisiin käyttää ylimmällä johdolla esimerkiksi johdon katselmuksessa ja saada mahdollisesti budjetti tarvittaville korjaustoimenpiteille.

6 Johtopäätökset/pohdinta

6.1 Jatkotoimenpiteet

Haastattelun ja havainnointini perusteella hedelmällisintä olisi tuottaa aiempi kysely uudelleen ja pitää Business Continuity council, samalla tapaa kuin yrityksessä pidetään IS council. Tällä varmistettaisiin riskianalyysin ja jatkuvuuden suunnitelman olevan mahdollisimman ajanmukainen ja yrityksen osastojen sisäinen vastausprosentti oletettavasti paljon korkeampi. Tällä saavutetaan laajempi yrityksen sisäinen tilannekuva ja riskimaisema. Silloin tiedetään teoriassa mahdollisista tilanteista osasto kohtaisella tasolla.

Havaintojen perusteella näkemykseni on, että mahdolliset riski tapahtumat voi jakaa kahteen eri luokkaan;

A. Tapahtuma, joka johtaa liiketoiminnan ja/tai sen kriittisten prosessien, joko kokonaiseen tai osittaiseen pysähtymiseen ja täten vaikuttaa yrityksen liiketoiminnan jatkuvuuteen ja yritystuottoon. A -luokan tapahtuman liiketoimi tappioita on mielestäni helpompi mitata, koska pysähtymiselle on näissä kyseisissä tapauksissa yleensä selvä alkamis- ja päättymisajankohta. *Erimerkki A -luokan tapahtumalle voisi olla huono käyttöjärjestelmäpäivitys, joka tulee suoraan toimittajalta ja sitä ei tietoturvakontrollit estä, tämän takia kaikki työasemat olisivat hetkellisesti käyttökelvottomia. Toinen esimerkki olisi yksinkertainen internet tai sähköpalveluntarjoajan kaatuminen.*

B. Työntekijä tason tapahtuma/ongelma, joka aiheuttaa työntekijäkohtaisia hidasteita päivittäisissä työtehtävissä. Tämä voi johtua tarvittavista resurssi puutteista ja on sama mitä yrityksen ISSO toteaa 4 kappaleessa. Työntekijän työtehokkuuden ylläpitämiseen tarvittava resurssit. Kyseinen tapahtuma ei suoranaisesti täysin pysäytä yrityksen liiketoimintaa, mutta hidastaa sen tuottoa sitä enemmän mitä kauemmin epäoptimaaliset prosessit käyvät yrityksessä. Tämä on mielestäni A-luokan tapahtumia petollisempi, koska useasti yritykset kantavat mukanaan vanhoja epäoptimoituja sisäisiä prosesseja ja näiden liiketappiota on sitä vaikeampi määritellä mitä kauemmin prosessi on käynyt. *Esimerkkinä työntekijä X kohtaa ongelman työasemallaan liiketoiminnalle kriittisen applikaation kanssa. Ongelmaa ei saada korjattua kuin vasta seuraavalla viikolla toimipisteitä kiertävän teknisen tuen vuoksi.*

6.2 Valittu viitekehys

Jälkikäteen miettiessäni valintaa ISO, COOP ja NIST väliltä on valinta ISO standardin suhteen ollut järkevin näin EU:n sisällä. NIST olisi ollut liian pitkä lähdepohjaksi, jonka takia aika ei olisi riittänyt. Oma mielipiteeni COOP suhteen on, että se on jokseenkin väärä ajattelumalli. Liiketoiminnan kannalta katsottuna, operations, eli yksi toiminto tai sen osa voi kaatua, mutta liiketoiminta silti jatkua. Tästä syystä mielipiteeni on, että laajempi liiketoiminnan jatkuvuuden hallinnan ajattelumalli on parempi kuin keskittyminen yksittäisiin toimintoihin. COOP toimintamalli keskittyy enimmäkseen kriittisestä tilasta palautumiseen, tätä voi verrata liiketoiminnan jatkuvuuden hallintajärjestelmän yhteen osioon, jatkuvuussuunnitelmaan, BCP. Toisinsanottuna COOP on vain pieni osa BCMS -hallintajärjestelmä kokonaisuudesta, BCP osio.

6.3 Omat tavoitteet

Oma tavoitteeni oli tuottaa mahdollisimman pitkälle kehitetty hallintajärjestelmän runko ja mielestäni tähän tavoitteeseen päästiin. Tarkoituksena ei ollut saada valmista hallintajärjestelmää kasattua yksin yrityksen ulkopuolelta. Tavoite, joka jäi saavuttamatta, oli suunnittelemani syvällisempi haastattelu ja sen tulokset yrityksen eri osastojen kanssa.

Isoimpana yllätyksenä tuli työn määrä, alusta saakka oli selvää, että pelkkä hallintajärjestelmän runko tulee olemaan iso työmäärä, mutta tarvittavien palojen yhdistyessä uutta työtä nousi jatkuvasti esille. Projektin aikana työn suunta muuttui hiukan haastattelujen ja sen painoarvon suhteen. Alku olettamasta poiketen soveltuvuuslausunnon ja Gap -analyysin painoarvo nousi oletettua suuremmaksi.

Jos saisin mahdollisuuden toistaa opinnäytetyöprosessin uudelleen, valitsisin ajanjakson siten, että työsuhde asiakasyrityksessä ei olisi lopuillaan opinnäytetyöprosessia aloittaessa.

6.4 Projektin loppuunsaattaminen ja prosessin käynnistäminen

Opinnäytetyöprosessin loppupuolella ja hallintajärjestelmä rungon ollessa valmis, arvioisin, että työtä pystyisi omatoimisesti saattamaan vielä noin 5-10% pidemmälle ilman yhteistyötä asiakasyrityksen kanssa. Nämä loput työt alkaisivat sisältämään arvailupohjaista toimintaa, joten en näe sen tuottavan mitään lisäarvoa itselleni tai asiakasyritykselle.

Tehty työ antaa arvioni mukaan noin 3-4 viikon työpanoksen projektiryhmältä, joka olisi kooltaan 2-3 henkilöä. Tästä huolimatta, oma ehdotukseni olisi laatia projekti suunnitelma ja aikataulu työtä jatkavalle ryhmälle. On myös otettava huomioon, että projektiryhmä tarvitsee oman aikansa tutkiessa valmiina olevaa materiaalia, jotta saavat niin sanotusti ”ajatuksesta kiinni”.

Oman kokemukseni perusteella, jos vertaan työmäärää ISO 27001 projektiin ja pidän mielessä siihen käytetyt työtunnit ja yrityskontekstin, määräisin projektille vähintään projektipäällikön ja yhden projektityöntekijän. Projektin loppuunsaattamiseen arvioisin kuluvan noin 3-6 kuukautta, riippuen lopullisesta projektiryhmä kokoonpanosta.

Isoimpana hankintana yritykselle näkisin uuden sijoituksen ja työroolin lisäämisen yritykseen. Uusi liiketoiminnan jatkuvuuden prosessi vastaava olisi parasta ottaa jo projekti vaiheessa tiiviisti mukaan, jotta perehdyttämiseltä vältyttäisiin.

Projektityön hyödynnettävyys on selvästi korkea, mutta mielestäni tulosten ja projektin levitettävyys, käyttö muussa kuin asiakasyrityksen kontekstissa, on hiukan alhaisempi. Tulokset ja arviot ovat suuresti sidoksissa yritys yhteistyökumppaniin, joten niitä voi olla vaikea hyödyntää muussa kontekstissa. Esimerkiksi luotu soveltuvuuslausunto ja siihen valitut kontrollit ja dokumentaatio on täysin tapauskohtainen.

Lähteet

Painetut

European Standard EN ISO 22301:2014 ”Societal security. Business continuity management systems. Requirements (ISO 22301:2012)”

Sähköiset

Business continuity planning, Wikipedia.org

https://en.wikipedia.org/wiki/Business_continuity_planning

The ISO 27001 & ISO 22301 Blog 2019, Rhand Leal

https://advisera.com/27001academy/blog/2019/12/02/iso-22301-2019-vs-iso-22301-2012-key-changes-infographic/

Kuviot

Kuvio 1: PDCA -menetelmän sykli. 11

Kuvio 2: Korkeantason projektisuunnitelma 13

Taulukot

Taulukko 1: Soveltuvuuslausunto **17**

Liitteet

Business Continuity Management System

Document

Internal

Table of contents

1 General ... 3
2 Business Continuity Management System scope ... 3
3 Information Security Competence ... 4
4 Information Security Policy ... 5
5 Asset management ... 5
6 Monitoring ... 5
7 Improvement ... 5
8 Risk Management System ... 5
9 Business Continuity Plan ... 5
10 ISMS Link ... 6
10.1 IT Disaster Recovery Plan ... 6
10.2 IT Service Continuity Plan ... 6
10.3 Information Security Procedures ... 6
10.4 Security Incident Management Process ... 6
11 Audits ... 6
12 Interested parties ... 7
13 Documentation control ... 7
14 Appendix ... 8
15 Version History ... 9
15.1 Reviewers and Approvals ... 9

About this Document

Purpose

This document describes the development of a Business Continuity Management System (BCMS) designed to ensure the recovery of critical business activities from natural or man-made failures or disasters to an acceptable level within a predefined time frame, thereby minimizing the impact of losses to the organization. Implementing a BCMS is essential for every business.

Intended Audience

Organisations IT division and all its business divisions

7 General

This document is determining external and internal issues that are relevant to the organization's information security management purpose and that affect its ability to achieve the intended outcome.

The purpose of this document is to define which information or business critical functions organization will protect with its BCMS (Business Continuity Management System). The document also describes the BCMS itself and what entities belongs to the management system.

Within BCMS documentation the group level organization Guidelines Framework's practices are used when applicable. Business continuity practical instructions are prepared and approved by X(TBA).

7.1 BCMS

Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

Business continuity management specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise

For organizations that wish to;

a) establish, implement, maintain and improve a BCMS,

b) ensure conformity with stated business continuity policy,

c) demonstrate conformity to others,

d) seek certification/registration of its BCMS by an accredited third-party certification body, or

e) make a self-determination and self-declaration of conformity with this International Standard

8 Business Continuity Management System scope

Business continuity program

Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.

Resources for this??(TBA)

Organization's Business Continuity Management System scope is set by evaluating the boundaries and applicability of the respective controls and considering interfaces and dependencies between activities performed by the organization and those that are performed by other organizations. The scope is re-evaluated regularly.

Organization will establish, implement, maintain and continually improve the Business Continuity Management System that will protect the organizations primary assets which are; Business processes & activities, information and supporting assets which are; Hardware, Software, Networks, Personnel, Physical sites and interested parties.

9 Analysis

9.1 Business Impact Analysis (BIA) + (Minimum business continuity objective)

9.2 Threat and risk analysis (TRA) (Data from the conducted study)

9.3 Impact scenarios (Data from the conducted study, if usable)

9.4 Recovery requirement (maximum acceptable outage, MAO) + (maximum tolerable period of disruption, MTPD) RPO + RTO

10 Personnel Competence

Role competences must be included in job descriptions and they are followed up by X(TBA) and other competence discussions with line manager.

AREA	Role	Competence
Workplace	Service owner	AV, WS FW, Endpoint protection, HD Encryption, Admin Rights, OS
Networks	Service owner	IDS/IPS, Proxy, FW, VPN, Active Devices, NetSec Architecture, Monitoring,
Data Center and Cloud	Service owner	Hardening, Server Certificate, Log Collection, AV, Encryption, OS, AD?
Mobile devices	Service owner	MDM, VPN, OS, Mobile Apps,
Identity and Access Management (IAM)	Service owner	IDM, AD, IAM Concept,
Collaboration Tools	Service owner	Office365, Spam Filter,
EUS	Service owner	Organization's Security Requirements,
SIAM	Service manager	Organization's Security Requirements,
Security Management	ISSO	ISMS, ISO27001, IAM, GDPR,
Applications	Application Senior manager	Citrix, IDM,
Internal audit	Auditor	27001 LA or Equivalent,
CRES	Auditor	Relevant IS competence depending on topic

11 Information Security Policy

Information Security Policy is a set of rules set by Organization's management to ensure that all users and information security structure within the organization's domain abide by the prescriptions regarding the security of information handling within the organization. The policy is approved by the CEO and it can be found as a separate document.

12 Asset management

Asset information is collected to asset inventory document and more detailed information could be found from separate databases. Respective asset owners are responsible for updating asset inventory whenever changes happen. Asset inventory can be found as a separate document.

13 Information Security Monitoring

Information security monitoring is divided into technical and administrative parts. Third party provider is providing regular technical security status reports. Administrative monitoring is performed according to ISMS requirements and followed up in management review meetings.

14 Improvement

Nonconformity and corrective actions

Nonconformities could be identified from different sources e.g. internal audits, technical audits, security incidents or interested party security notification.

Organization will evaluate nonconformities according to their nature and relevance to Organization's environment.

Service owner is making root cause analysis basing on information about e.g. cause, coverage and escalation potential. Corrective Action Template population is started according to identified information.

Service owner in accordance with the process owner design the correction plan. Service owner drive corrective actions with respective partners.

Service owner make effectiveness verification when corrective action is in use.

Service owner, ISSO and relevant suppliers will evaluate preventive actions to e.g.BCMS, ISMS or technical solutions.

15 Risk Management System

Risk management system is a management system that assists in consolidating asset values, claims, policy, and exposure of information and providing the tracking and management reporting capabilities to enable the management to monitor and control the overall risk management posture. Risk management system can be found as a separate documentation.

16 Business Continuity Plan

A Business Continuity Plan outlines a range of disaster scenarios and the steps the business will take in any particular scenario to return to regular trade.

Business continuity planning (BCP) is the creation of a strategy through the recognition of threats and risks intent to the Organization (Conducted study material). The purpose is to ensure that personnel and assets are protected and able to function in the event of a disaster. The plan can be found as a separate document.

17 ISMS Link

17.1 IT Disaster Recovery Plan

Disaster recovery plan (DRP) is a documented process of procedures to recover and protect a business IT infrastructure in the event of a disaster. The plan specifies procedures an organization is to follow in the event of a disaster. The plan can be found as a separate document.

17.2 IT Service Continuity Plan

IT Service Continuity is a subset of Business Continuity Planning (BCP) and encompasses IT disaster recovery planning and wider IT resilience planning. It also incorporates those elements of IT infrastructure and services. The plan can be found as a separate document.

17.3 Information Security Procedures

The goal of Information Security Procedures is to limit information access to authorized users, protect information against unauthorized modification, and ensure that information is accessible when needed. The procedures plan can be found as a separate document.

17.4 Security Incident Management Process

In collaboration with third party provider its function is to filter the security events and process the actual security incidents. The process is done by the provider and the collected data is then presented to Organization’s Information Systems Security Officer. The process is documented and can be found as a different file separate to this.

18 Audits

Main information security audits are conducted by internal audits, which are included in the Organization’s IT division internal audit program. Each information security internal audit is planned separately by the internal auditor.

Technical audits are taking place according to the annual audit plan conducted by external auditor. The external auditor will prepare respective audit reports and development actions.

Third party provider will run regular vulnerability scans to Organization’s environment and execute corrective actions.

19 Interested parties

Organization has defined relevant internal and external interested parties which are important for Organization's ISMS utilization. The main documents to control interested parties' security compliance are Non-disclosure Agreements (NDA), Minimum Security Requirements, Cloud Security Requirements and Information Security Policy. These documents can be found as separate files.

The owners for each interested party have been nominated and they are responsible for communication establishment and utilization.

Interested party coverage is evaluated by risk management process.

20 Documentation control

Organization has defined general documentation management principles. They include e.g. documentation classification, availability, suitability for use, adequate protection, control of changes and disposal. More detailed information is found as a separate file.

21 Appendix

Table 1 List of Abbreviations

Abbreviation	Expansion
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
ISMS	Information Security Management System
IM	Incident Management
ISSO	Information Systems Security Officer
ITSM	IT Service Management
SIAM	Service Integration and Management

22 Version History

Version	Date	Prepared by	Approved by	Changes
0.1	26.10.2018	Juuso Hirsmäki		First draft and main titles
0.2	2019	Juuso Hirsmäki		Updates + additions
0.3	09.03.2020	Juuso Hirsmäki		Red marks, need for censorship in the final version.
				-
				-
				-
				-
				-
				-
				-

22.1 Reviewers and Approvals

This document requires the following reviews and approvals.

Name	Signature on approval	Date	Version
Steering group		End of Preparation phase: xx xx	1.0
Business Owner of the project		End of closing phase: xx xx	2.0

Direction: you should follow the listed procedure in versioning the document:

- Document created = version 0.1.x
- Draft = 0.2.X….0.9 X
- Document approved in the end of Preparation phase by the Steering Group = 1.0 (Investment approval/Gate 1)
- Document approved by the Business Owner/Steering group in the end of project (Business owner approval/Gate 5) = 2.0.

Business Continuity Plan

Internal

About this Document

Purpose

This document describes the development of a Business Continuity Plan (BCP) designed to ensure the recovery of critical business activities from natural or man-made failures or disasters to an acceptable level within a predefined time frame, thereby minimizing the impact of losses to the organisation. Implementing a BCP is essential for every business.

Intended Audience

Organization’s Group IT and all its business divisions

Contents

1. GENERAL....13
2. FIVE MAJOR PROCESSES....13
3. BUSINESS IMPACT ANALYSIS (BIA)....14
4. THREAT AND RISK ANALYSIS (TRA)....14
5. IMPLEMENTATION....14
6. RECOVERY STRATEGIES....15
7. Document Control....16
8. Appendix....16
9. Abbrevations....16

x

1. GENERAL

Business continuity planning (BCP) is the creation of a strategy through the recognition of threats and risks facing a company, with an eye to ensure that personnel and assets are protected and able to function in the event of a disaster.
Business continuity planning involves defining potential risks, determining how those risks will affect operations, implementing safeguards and procedures designed to mitigate those risks, testing those procedures to ensure that they work, and periodically reviewing the process to make sure that it is up to date.

High level tasks

- Deciding the criteria triggering the plan (Company decision, TBA)
- Determine the scope of the BCP (Top level management decision, which process owner shall follow through)
- Classification of various security incidents (Company/BCMS responsible person decision, TBA)
- Employee roles and responsibilities (Company decision, TBA)
- Gain executive support (ISO 22301 requirement)
- Evaluate your incident response plan
- Test your plan (Run a Proof of Concept, POC, before the go-live)

2. FIVE MAJOR PROCESSES

3. BUSINESS IMPACT ANALYSIS (BIA)

A Business impact analysis (BIA) differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function may also be considered critical if dictated by law. For each critical (in scope) function, two values are then assigned:

- Recovery Point Objective (RPO) – the acceptable latency of data that will not be recovered. For example, is it acceptable for the company to lose 2 days of data?
- Recovery Time Objective (RTO) – the acceptable amount of time to restore the function.

The recovery point objective must ensure that the maximum tolerable data loss for each activity is not exceeded. The recovery time objective must ensure that the Maximum Tolerable Period of Disruption for each activity is not exceeded.

Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

- The business requirements for recovery of the critical function, and/or
- The technical requirements for recovery of the critical function

4. THREAT AND RISK ANALYSIS (TRA)

After defining recovery requirements, each potential threat may require unique recovery steps. Common threats include:

- Fire
- Cyber attack
- Sabotage (internal or external)
- Power outage
- Telecommunications outage
- IT outage
- Theft (internal or external threat, vital information or material)
- Random failure of mission-critical systems
- Single point dependency

5. IMPLEMENTATION

The implementation phase involves policy changes, material acquisitions, staffing and testing.

6. RECOVERY STRATEGIES

If a facility is damaged, production machinery breaks down, a supplier fails to deliver or information technology is disrupted, business is impacted, and the financial losses can begin to grow. Recovery strategies are alternate means to restore business operations to a minimum acceptable level following a business disruption and are prioritized by the recovery time objectives (RTO) developed during the business impact analysis.

Recovery strategies require resources including people, facilities, equipment, materials and information technology. An analysis of the resources required to execute recovery strategies should be conducted to identify gaps. For example, if a system fails but other systems are readily available to make up lost processing, then there is no resource gap.

7. Document Control

Date	
Approved by	
Document type	Process Description
Document owner	Information Systems Security Officer

Version	Date	Description	Responsible
0.1.	12.11.2018	Initial version	Juuso Hirsmäki
0.2	2019	updates	Juuso Hirsmäki
0.2	09.03.2020	Red marks, needs censorship in the final version	Juuso Hirsmäki
1.0		CIO and ITLM approval	

8. Appendix

9. Abbrevations

BCP	Business Continuity Plan
SDM	Service Delivery Manager
SOC	Security Operation Center
ISSO	Information Systems Security Officer
SLA	Server Level Agreement
SD	Service Desk

Table 2 List of Abbreviations

Abbreviation	Expansion
CI	Configuration Item
CM	Change Management
CMDB	Configuration Management Database
IM	Incident Management
IT	Information Technology
ITSM	IT Service Management
MIM	Major Incident Management
OLA	Operational Level Agreements
PM	Problem Management
POC	Point Of Contact
RFC	Request For Change

SIAM	Service Integration and Management
SLA	Service Level Agreements

Statement of Applicability Current version 0.1 as of: 09/03/2020

Legend (for Selected Controls and Reasons for controls selection)

LR: **legal requirements,**CO: **contractual obligations,**BR/BP: **business requirements/adopted best practices,**RRA: **results of risk assessment(Reference to risk analysis numbering),**TSE: to some extent

	ISO 22301 : 2014 "Societal security. Business continuity management systems."		Current control	Selected controls and reasons for selection				Source Reference/ Reason for inclusion / exclusion	Documentation requirement + Status	Status
				LR	CO	BR/BP	RRA			
Chapter	Title/Description	Control Description/Reference								
0.1	Policy	PDCA -cycle or equivalent			?	x				Documentation missing
0.1	Objectives	Included in policy				x				Documentation missing
0.1	People with defined responsibilities	Included in policy				x				Documentation missing
0.1	Planning									Documentation missing
0.1	Implementation and operation					x				Documentation missing
0.1	Performance assessment					x				Documentation missing
0.1	Management review					x				Documentation missing
0.1	Improvement					x				Documentation missing
0.2	Plan, Do, Check, Act cycle implemented	Included in policy?				x				Documentation missing
3.2	Audit documentation			x?		x			0%	Documentation missing
3.6	Business Continuity Plan				x?	x				BCP draft done
4.1	Understandin the organization and its context									Will be included in BCMS documentation
	a) activities, functions, services, products, partnerships, supply chains, relationships with interested parties and the potential impact related to a disruptive incident									Will be included in BCMS documentation
	b) Links between the BC Policy and organizations objectives and other policies, including its overall risk management strategy									Will be included in BCMS documentation
	c) the organizations risk appetite									Will be included in BCMS documentation
4.1	Establishing the cotnext, the organization shall;									Will be included in BCMS documentation
	1) articulate its objectives,(concerned with BC)									Will be included in BCMS documentation
	2) define external/internal factors that create the uncertainty that gives rise to risk									Will be included in BCMS documentation
	3) set risk criteria taking into account the risk appetite									Will be included in BCMS documentation
	4) define the purpose of the BCMS									Found in BCMS documentation
4.2.2	Legal and regulatory requirements	Included in policy?		x		x				Documentation missing
	The organization shall establish, implement and maintain a procedure to identify, have access to, and assess the applicable legal and regulatory requirements... The organization shall document this information.			x		x			0%	Documentation missing
4.3	Determining the scope of the business continuity management system					x				Will be included in BCMS documentation
4.3.1	General									Documentation missing
	The organization shall determine the boundaries and applicability of the BCMS to establish its scope. The scope shall be available as documented information.					x			20%	Documentation missing, top level management decisio
4.3.2	Scope of the BCMS					x				BCMS draft done
	When defining the scope, the organization shall document and explain exclusions, these shall not affect the organisation's ability and responsibility to provide continuity on business and operations.									BCMS draft done
5.2	Management commitment					x				Management review not done
	Top management shall demonstrate leadership and commitment with respect to the BCMS by					x				Management review not done
	a) Ensuring that policies and objectives are compatible and aligned with strategic direction of the organisation					x				Management review not done
	b) Ensuring integration of business continuity management requirements into the organisation's business processes					x				Management review not done
	c) Allocating needed resources									Management review not done
	d) Communicating the importance of effective business continuity management and conforming to the BCMS requirements					x				Management review not done
	e) Ensuring that the BCMS achieves its intended outcomes					x				Management review not done
	f) Directing and supportin g persons to contribute to the effectiveness of the BCMS					x				Management review not done
	g) Promoting continual improvement, and					x				Management review not done
	h) Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility					x				Management review not done
	Top management shall provide evidence of this commitment to the BCMS by					x				Documentation missing, Management review not done
	a) Establishing business continuity policy					x				Management review not done
	b) Ensuring that BCMS objectives and plans are established					x				Management review not done
	c) Establishing roles, responsibilities, and competencies for business continuity management, and					x				Management review not done
	d) Appointing one or more persons to be responsible for the BCMS with appropriate authority and competencies					x				Management review not done

5.3	Policy									Documentation missing
	Top management shall establish a business continuity policy that					x				Management alignment not done
	a) Is appropriate to the purpose of the organization				x?	x				Management review not done
	b) Provides a framework for setting business continuity objectives					x				Management review not done
	c) Includes a commitment to satisfy applicable requirements					x				Management review not done
	d) Includes a commitment to continual improvement of the BCMS					x				Management review not done
	The BCMS policy shall									Will be included in BCMS documentation
	a) Be available as documented information					x			0%	Will be included in BCMS documentation
	b) Be communicated within the organisation					x				Will be included in BCMS documentation
	c) Be available to interested parties, as appropriate					x				Will be included in BCMS documentation
	d) Be reviewed for continuing suitability at defined intervals and when signifigant changes occur					x				Will be included in BCMS documentation
5.4	Organisational roles, responsibilities and authorities									Documentation missing, included in BC Policy
	Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organisation					x				Documentation missing, included in BC Policy
	Top management shall assing the responsibility and authority for					x				Documentation missing, included in BC Policy
	a) Ensuring that the management system conforms to the requirements of the international standard (ISO 22301)					x				Documentation missing, included in BC Policy
	b) Reporting on the performance of the BCMS to top management					x				Documentation missing, included in BC Policy
6.2	Business continuity objectives and plans to achieve them									Will be included in BCP documentation
	Top management shall ensure that business continuity objectives are established and communicated					x				Will be included in BCP documentation
	The business continuity objectives shall									Will be included in BCP documentation
	a) Be consisten with the business continuity policy					x				Will be included in BCP documentation
	b) Take account of the minimun level of products and services that is acceptable to the orgaanisation to achieve its objectives					x				Will be included in BCP documentation
	c) Be measurable					x				Will be included in BCP documentation
	d) Take into account applicable requirements, and					x				Will be included in BCP documentation
	e) Be monitored and updated as appropriate					x				Will be included in BCP documentation
	The organisation shall retain documented information on the business continuity objectives					x			50%	Will be included in BCP documentation
	To achieve its business continuity objectives, the organisation shall determine									Will be included in BCP documentation
	a) Who will be responsible					x				Will be included in BCP documentation
	b) What will be done									Will be included in BCP documentation
	c) What resources will be required					x				Will be included in BCP documentation
	d) When it will be completed, and					x				Will be included in BCP documentation
	e) How the results will be evaluated					x				Will be included in BCP documentation
7.2	Competence					x				Found in BCMS documentation
	The organisation shall									Found in BCMS documentation
	a) Determine the necessary competence of persons working with the BCMS					x				Found in BCMS documentation
	b) Ensure that these persons are competent on the basis of appropriate education, training, and expertice					x				Found in BCMS documentation
	c) Where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken, and					x				Found in BCMS documentation
	d) Retain appropriate documented information as evidence of competence					x			80%	Found in BCMS documentation
7.5	Documented information					x			40%	Will be included in BCMS documentation
7.5.2	Creating and updating					x				Will be included in BCMS documentation
	When creating and updating documented information, the organisation shall ensure appropriate					x				Will be included in BCMS documentation
	a) Identification and description (title, date, author or reference number)					x				Will be included in BCMS documentation
	b) Format (Language, software version, graphics) and media (Paper, electronic), and review and approval for suitability and adequacy					x				Will be included in BCMS documentation
7.5.3	Control of documented information					x			70%	Will be included in BCMS documentation, version contr
	Documented information required by the BCMS and by ISO22301 shall be controlled to ensure									Will be included in BCMS documentation, version contr
	a) It is available and suiteble for use, where and when it is needed,					x				Will be included in BCMS documentation, version contr
	b) It is adequately protected (From loss of confidentiality, improper use, or loss of integrity)					x				Will be included in BCMS documentation
	For the control of documented information, the organisation shall adress the following activities, as applicable									Will be included in BCMS documentation
	a) Distribution, access, retrievall and use					x				Will be included in BCMS documentation
	b) Storage and preseervation, including preservation of lagibility					x				Will be included in BCMS documentation
	c) Control of changes (Version control)					x				Will be included in BCMS documentation

	d) Retention and disposition					x				Will be included in BCMS documentation
	e) Preservation of legibility (Clear enough to read), and					x				Will be included in BCMS documentation
	f) Prevention of the unintended use of obsolete information					x				Will be included in BCMS documentation
8	Operation									BCMS draft done + BCP
8.1	Operational planning and control					x				BCMS draft done + BCP
	The organisation shall plan, implement and control the processes needed to meet requirements by					x				BCMS draft done + BCP
	a) Establishing criteria for the processes					x				Documentation missing
	b) Implementing control of the processes in accordance with the criteria, and					x				Documentation missing
	c) Keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned					x			0%	Documentation missing
8.2	Business impact analysis and risk assessment					x				BCMS draft done + BCP
8.2.1	General									BCMS draft done + BCP
	The organisation shall establish, implement and maintain a formal and documented process for business impact analysis and risk assessment that					x			80%	BCMS draft done + BCP
	a) Establishes the context of the assessment, defines criteria and evaluates the potential impact of a disruptive incident					x				BCMS draft done + BCP
	b) Takes into account legal and other requirements to which the organisation subscribes			x		x				Documentation missing
	c) Includes systematic analysis, priorization of risk treatments and their related costs					x				Documentation missing
	d) Defines the required output frpm the business impact analysis and risk assessment and					x				Documentation missing
	e) Specifies the requirements for this information to be kept up to date and confidential					x				BCMS draft done + BCP
8.2.2	Business impact analysis					x				BCMS draft done + BCP
	The organisation shall establish, implement and maintain a formal and documented evaluation process for determining continuity and recovery priorities, objectives and targets					x			80%	BCMS draft done + BCP
	The business impact analysis shall include the following:									BCMS draft done + BCP
	a) Identifying activities that support the provision of products and services					x				TBA, process owner/management decision
	b) Assessing the impacts over time of not performing these activities					x				TBA, process owner/management decision
	c) Setting prioritized timeframes for resuming these activities at specified minimum acceptable level, taking into consideration the time within which the impact of not seruming them would become unacceptable, and					x				TBA, process owner/management decision
	d) Identifying dependencies and supporting resources for these activities, including suppliers, outsource partners and other interested parties					x				TBA, process owner/management decision
8.2.3	Risk assessment					x				Risk landscape to be determined, BC Council to be held
	The organization shall establish, implement, and maintain a formal documented risk assessment process that systematically identifies, analyses and evaluates the risk of disruptive incidents to the organisation					x			60%	Documentation missing
	The organization shall									Risk landscape to be determined, BC Council to be held
	a) Identify risks of disruption to the organization's prioritized activities and processes, systems, information, people, assets, outsource partners and other resources that support them					x				Risk landscape to be determined, BC Council to be held
	b) Systematically analyse risks					x				Risk landscape to be determined, BC Council to be held
	c) Evaluate which disruption related risks require treatment, and					x				Risk landscape to be determined, BC Council to be held
	d) Identify treatments commensurate with business continuity objectives and in accordance with the organisation's risk appetite					x				Risk landscape to be determined, BC Council to be held
8.3	Business continuity strategy	Included in policy?				x				Documentation missing
8.3.1	Determination and selection	Included in policy?								Documentation missing
	The organisation shall determine an appropriate business continuity strategy for	Included in policy?				x				Documentation missing
	a) Protecting prioritized activities	Included in policy?				x				Documentation missing
	b) Stabilizing, continuing, resuming and recovering prioritized activities and their dependencies and supporting resources, and	Included in policy?				x				Documentation missing
	c) Mitigating, responding to and managing impacts	Included in policy?				x				Documentation missing
8.3.2	Establishing resource requirements	Included in policy?				x				Documentation missing
	The organisation shall determine the resource requirements to implement the selected strategies. The types of resources considered shall include but not be limited to	Included in policy?				x				Documentation missing
	a) People	Included in policy?								Documentation missing
	b) Information and data	Included in policy?								Documentation missing
	c) Buildings, work environment and associated utilities	Included in policy?								Documentation missing
	d) Facilities, equipment and consumables	Included in policy?								Documentation missing
	e) Information and communication technology (ICT) systems	Included in policy?								Documentation missing
	f) Transportation	Included in policy?								Documentation missing
	g) Finance, and	Included in policy?								Documentation missing
	h) Partners and suppliers	Included in policy?								Documentation missing
8.3.3	Protection and mitigation	Included in policy?								Documentation missing
	For identified risks requiring treatment, the organisation shall consider proactive measures that	Included in policy?				x				Documentation missing
	a) Reduce the likelihood of disruption	Included in policy?				x				Documentation missing

x

	b) Shorten the period of disruption, and	Included in policy?				x				Documentation missing
	b) Limit the impact of disruption on the organisation's key products and services	Included in policy?				x				Documentation missing
8.4	Establish and implement business continuity procedures	Included in policy?				x				Documentation missing
8.4.1	General	Included in policy?								Documentation missing
	The organisation shall establish, implement and maintain business continuity procedures to manage a disruptive incident and continue its activities based on recovery objectives identified in the business impact analysis	Included in policy?				x				Documentation missing
	The organisation shall document procedures (including necessary arrangements) to ensure continuity of activities and management of disruptive incident	Included in policy?				x			40%	Documentation missing
	The Procedures shall	Included in policy?								Documentation missing
	a) Establish an appropriate internal and external communications protocol	Included in policy?				x				Documentation missing
	b) Be specific regarding the immediate steps that are to be taken during disruption	Included in policy?				x				Documentation missing
	c) Be flexible to respond to unanticipated threats and changing internal and external conditions	Included in policy?				x				Documentation missing
	d) Focus on the impact of events that could potentially disrupt operations	Included in policy?				x				Documentation missing
	e) Be developed based on stated assumptions and an analysis of interdependencies, and	Included in policy?				x				Documentation missing
	f) Be effective in minimizing consequences through implementation of appropriate mitigation strategies	Included in policy?				x				Documentation missing
8.4.2	Incident response structure	To be included in BCP/BCMS document?								Documentation missing
	The organisation shall establish, document, and implement procedures and management structure to respond to disruptive incident using personnel with the necessary responsibility, authority and competence to manage an incident	To be included in BCP/BCMS document?				x			0%	Documentation missing
	The response structure shall	To be included in BCP/BCMS document?								Documentation missing
	a) Identify impact tresholds that justify initiation of formal response	To be included in BCP/BCMS document?				x				Documentation missing
	b) Assess the nature and extent of disruptive incident and its potential impact	To be included in BCP/BCMS document?				x				Documentation missing
	c) Activate and appropriate business continuity response	To be included in BCP/BCMS document?				x				Documentation missing
	d) Have processes and procedures for the activation, operation, coordination and communication of the response	To be included in BCP/BCMS document?				x				Documentation missing
	e) Have resouces available to support the processes and procedures to manage a disruptive incident in order to minimize impact, and	To be included in BCP/BCMS document?				x				Documentation missing
	f) Communicate with interested parties and authorities, as well as the media	To be included in BCP/BCMS document?				x				Documentation missing
8.4.4	Business continuity plans					x				Documentation missing
	Each plan shall define									Documentation missing
	a) Purpose ands cope	To be included in BCP/BCMS document?				x				Documentation missing
	b) Objectives	To be included in BCP/BCMS document?				x				Documentation missing
	c) Activation criteria and procedures	To be included in BCP/BCMS document?				x				Documentation missing
	d) Implementation procedures	To be included in BCP/BCMS document?				x				Documentation missing
	e) Roles, responsibilities and authorities	To be included in BCP/BCMS document?				x				Documentation missing
	f) Communication requirements and procedures	To be included in BCP/BCMS document?				x				Documentation missing
	g) Internal and external interdependencies and interactions	To be included in BCP/BCMS document?				x				Documentation missing
	h) Resource requirements, and	To be included in BCP/BCMS document?				x				Documentation missing
	I) Information flow and documentation processes	To be included in BCP/BCMS document?				x				Documentation missing
8.4.5	Recovery	To be included in BCP/BCMS document?								Documentation missing
	The organisation shall have documented procedures to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident	To be included in BCP/BCMS document?				x			0%	Documentation missing
8.5	Exercising and testing									Documentation missing
9	Performance evaluation	To be included in BCP/BCMS document?				x				Documentation missing
9.1	Monitoring, measurement, analysis and evaluation	Third party metrics service?				x				Documentation missing
9.1.1	General									Documentation missing
	The organisation shall determine	Third party metrics service?								Documentation missing
	a) What needs to be monitored	Third party metrics service?				x				Documentation missing
	b) The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results	Third party metrics service?				x				Documentation missing
	c) When the monitoring and measuring shall be performed, and	Third party metrics service?				x				Documentation missing
	d) When the results from monitoring and measurement shall be analysed and evaluated	Third party metrics service?				x				Documentation missing
	The organisation shall retain appropriate documented information as evidence of the results	Third party metrics service?				x			0%	Documentation missing
9.1.2	Evaluation of business continuity procedures	To be included in BCP/BCMS document?				x				Documentation missing
9.2	Internal audit	Internal BC audit plan				x				Documentation missing
	The organisation shall conduct internal audits at planned intervals to provide information on whether the business contunuity management system	Internal BC audit plan				x				Documentation missing
	a) Confoms to	Internal BC audit plan								Documentation missing
	1. The organisation's own requirements for its BCMS,	Internal BC audit plan				x				Documentation missing

	2. The requirements of ISO22301, and	Internal BC audit plan				x				Documentation missing
	b) Is effectively implemented and maintained	Internal BC audit plan				x				Documentation missing
	The organisation shall	Internal BC audit plan								Documentation missing
	a) Plan, establish, implement and maintain an audit programme, including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme shall take into consideration the importance of the processes concerned and the results of previous audits	Internal BC audit plan				x				Documentation missing
	b) Define the audit criteria and scope for each audit	Internal BC audit plan				x				Documentation missing
	c) Select auditors and conduct audits to ensure objectivity and impartiality of the audit process	Internal BC audit plan				x				Documentation missing
	d) Ensure that the results of the audits are reported to relevant management, and	Internal BC audit plan				x				Documentation missing
	e) Retain documented information as evidence of the implementation of the audit programme and the audit results	Internal BC audit plan				x			0%	Documentation missing
	The audit programme shall be based on the results of risk assessment and results of previous audits.	Internal BC audit plan				x				Documentation missing
9.3	Management review					x				Documentation missing, Management review not done
	Top management shall review the organisation's BCMS, et planned intervals, to ensure its continuing suitability, adequacy and effectiveness.					x				Documentation missing, Management review not done
	The management review shall include consideration of									Documentation missing, Management review not done
	a) The status of actions from previous management review,					x				Documentation missing, Management review not done
	b) Changes in external and internal issues that are relevant to the business continuity management system,					x				Documentation missing, Management review not done
	c) Information on the business continuity performance, including trends in					x				Documentation missing, Management review not done
	1. Nonconformities and corrective actions,					x				Corrective actions draft done
	2. Monitoring and measurement evaluatin results, and					x				Documentation missing, Management review not done
	3. Audit results					x				Documentation missing, Management review not done
	d) Opportunities for continual improvement					x				Documentation missing, Management review not done
10	Improvement									Documentation missing
10.1	Nonconformity and corrective action					x				Corrective actions draft done
	When nonconformity occurs, the organisation shall									Corrective actions draft done
	a) Identyfy the nonconformity					x				Corrective actions draft done
	b) React to the nonconformity, and, as applicable					x				Corrective actions draft done
	1. Take action to control and corret it					x				Documentation missing
	2. Deal with the consequences					x				Documentation missing
	c) Evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by					x				Documentation missing
	1. Reviewing the nonconformity					x				Documentation missing
	2. Determining the causes of the nonconformity, and					x				Documentation missing
	3. Determining of similar nonconformities exist, or could potentially occur,					x				Documentation missing
	4. Evaluating the need for corrective action to ensure that nonconformities do not recur or occur elsewhere,					x				Corrective actions draft done
	5. Determining and implementing corrective action needed,					x				Corrective actions draft done
	6. Reviewing the effectiveness of any corrective action taken and					x				Corrective actions draft done
	7. Making changes to the BCMS, if necessary					x				Documentation missing
	d) Implementing any action needed					x				Corrective actions draft done
	e) Review the effectiveness of any corrective action taken					x				Corrective actions draft done
	f) Make changes to the BCMS, if necessary					x				Documentation missing
	Corrective actions shall be appropriate to the effects of the nonconformities encountered					x				Corrective actions draft done
	The organisation shall retain documented information as evidence of					x			60%	Corrective actions draft done
	1. The nature of the nonconformities and any subsequent actions taken, and					x				Corrective actions draft done
	2. The results of any corrective action					x				Corrective actions draft done
10.2	Continual improvement					x				Documentation missing
	The organisation shall continually improve the suitability, adequacy or effectiveness of the BCMS					x				Documentation missing

Documentation requirement	Status	
Legal and regulatory requirements, The organization shall establish, implement and maintain a procedure to identify, have access to, and assess the applicable legal and regulatory requirements	0%	Documentation missing
BCMS scope documentation	20%	Documentation missing, top level management decision/process owner proposal
BCMS Policy shall be available as documented information	0%	Will be included in BCMS documentation
Documented business continuity objectives	50%	Will be included in BCP documentation
Documented information of personnel competence	80%	Found in BCMS documentation
Documented information about documentation processes	80%	Will be included in BCMS documentation, version control, management review and approval cycle already in place
Control of documented information	70%	Will be included in BCMS documentation, version control, management review and approval cycle already in place
Keeping documented information about operational planning and processes to the extent necessary to have confidence that the processes have been carried out as planned	0%	Documentation missing
The organisation shall establish, implement and maintain a formal and documented process for business impact analysis and risk assessment that	80%	BCMS draft done + BCP
BIA, The organisation shall establish, implement and maintain a formal and documented evaluation process for determining continuity and recovery priorities, objectives and targets	80%	BCMS draft done + BCP
The organization shall establish, implement, and maintain a formal documented risk assessment process that systematically identifies, analyses and evaluates the risk of disruptive incidents to the organisation	60%	BCP documentation, BIA, TRA + BC Council?
The organisation shall document business continuity procedures (including necessary arrangements) to ensure continuity of activities and management of disruptive incident	40%	Documentation WIP
Incident response structure, The organisation shall establish, document, and implement procedures and management structure to respond to disruptive incident using personnel with the necessary responsibility, authority and competence to manage an incident	0%	Documentation missing
Recovery, The organisation shall have documented procedures to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident	0%	Documentation missing
Monitoring, measurement, analysis and evaluation, The organisation shall retain appropriate documented information as evidence of the monitoring and measurement results	0%	Documentation missing
Internal audit, Conpany shall retain documented information as evidence of the implementation of the audit programme and the audit results	0%	Documentation missing
Improvement, Nonconformities and corrective action. The organisation shall retain documented information as evidence of the nature of the nonconformities and any subsequent actions taken, and the results of any corrective action	60%	Corrective actions draft done
Average:	**36%**	